PERSONNEL CABINET
DEPARTMENT OF EMPLOYEE INSURANCE
HIPAA SECURITY POLICIES AND PRACTICES

I. Administrative Safeguards

A. Assign Security Responsibility

The Commissioner, Department of Employee Insurance, shall identify a Security Official who is responsible for the development and implementation of the required policies and procedures.

The Security Official is responsible for the development and implementation of the required policies and procedures is the branch manager of the Data Analysis Branch. The branch manager reports directly to the Commissioner's Office. The Security Officer will work in conjunction with the Office of Legal Services and Division of Technology Services within the Personnel Cabinet in the development and maintenance of the HIPAA Security policies and procedures.

The Security Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their E-PHI. The Security Official is responsible for creating a process for individuals to lodge complaints about the Plan's security procedures and for creating a system for handling such complaints.

B. Training of Workstation Use

DEI shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes or the surroundings of a specific workstation or class of workstations that can access E-PHI.

C. Workforce Security

DEI shall ensure that all members of its workforce have access to E-PHI appropriate to the duties of the workforce member and to prevent those workforce members who should not have access to E-PHI from obtaining access. DEI's workforce security shall include the following: The Security Official shall train all staff regarding HIPAA Security requirements as it pertains to their specific job duties.

The Security Official is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their functions with the Plan.

All employees and Insurance Coordinator's and Associate Insurance Coordinator's receive annual HIPAA trainings. All new employees shall be trained within thirty (30) days of hire date. All new Insurance Coordinator's and Associate Insurance Coordinator's shall be trained on HIPAA within thirty (30) days of such designation. All employees or Insurance Coordinator's or Associate Insurance Coordinator's that do not complete HIPAA training have their access terminated.

1. Authorization and/or Supervision

DEI shall implement procedures for the authorization and/or supervision of workforce members who work with E-PHI or who work in location where it might be accessed.

There are four applications supporting the Health Plan including the Group Health Insurance (GHI) database, the Premium Bill and Reconciliation (PB&R) database, Web Billing and Web Enrollment and all are protected by login IDs and passwords. The levels of access to E-PHI range from read-only to complete system access with the ability to change specific individual's E-PHI. Only select management staff determines user access levels which are then maintained via a security table within the database (Table Maintenance). The user ID and password are stored within Table Maintenance, which may be updated only by specific DEI staff with system DEI access.

As a covered entity, DEI has endeavored to completely document their HIPAA security compliance in a more detailed document for granting system access. Therefore, highly sensitive procedures used by staff have been limited here to prevent unauthorized access to E-PHI. 2. Workforce Clearance Procedure

DEI shall determine that a workforce member's access to E-PHI is appropriate.

Management staff is responsible for determining the level of access granted to staff based on their job duties. Every employee of DEI will access E-PHI at some measure in their daily job functions.

3. Termination Procedures

DEI shall have a process for terminating access to E-PHI when the employment of a workforce member ends or when it is determined that it is not appropriate for certain workforce members to have access to E-PHI. Upon termination, all user access is revoked immediately within Table Maintenance and Network Support

staff is notified to immediately revoke system-wide user access. All keys and security ID badges will be turned in to the immediate supervisor.

II. System Safeguards

A. Workstation Security

DEI shall have physical safeguards for all workstations that access E-PHI, in order to restrict access to authorized users.

All workstations automatically lock-out after ten (10) minutes. All screens must not face an open door. DEI shall, on behalf of the Plan, ensure that the appropriate technical and physical safeguards to prevent E-PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls.

B. Security Management Process

DEI shall prevent, detect, contain, and correct security violations. The Security Management Process shall include the following:

1. Risk Analysis Annually, DEI shall conduct an accurate and thorough assessment of the potential risk and vulnerabilities to the confidentiality, integrity, and availability of E-PHI.

2. Risk Management

   DEI shall implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level.

   DEI will conduct an updated risk analysis each February and August in order to determine its continued compliance with HIPAA. As part of DEI's risk management, DEI compiled these policies and procedures which outline all the requirements of the HIPAA Security Rule.

3. Sanction Policy
   DEI shall apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures.

   Sanctions for using or disclosing E-PHI in violation of the HIPAA Security Policies and Procedures may be imposed against any employee, including but not limited to, termination of employment.

4. Information System Activity Review

   DEI shall regularly review records of information system activity, such as

audit logs, access reports, and security incident tracking reports. Quarterly assessments are completed by third party vendors.

C. Information Access Management

DEI shall implement policies and procedures for authorizing appropriate access to E-PHI. The policies and procedures shall include the following:

1. Access Authorization

DEI shall implement policies and procedures for granting access to E-PHI.

To prevent unauthorized access, all employees of DEI must provide a unique ID and password when logging into their computer for system wide access. This level of security is maintained by Network Support. In addition, to log into the GHI and PB&R databases a second ID and password are required. This security is maintained via Table Maintenance.

2. Access Establishment and Modification

Based upon the entity's access authorization policies, DEI shall establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. Initial user access is established by Management Staff upon initial hiring. User access levels are modified on an "as needed" basis when changes in job responsibilities necessitate such action.

D. Protection from Malicious Software

DEI shall address how it will implement procedures that will guard against and detect and report malicious software (e.g. viruses or a virus reminder).

Network Support staff uses McAfee Virus Scan. This protects the SQL server and all workstations and it is updated every workday. DEI's systems are also protected by a firewall within the Personnel Cabinet as well as one provided by the Commonwealth Office of Technology. The firewall is a hardware/software application and it protects against any unauthorized access to out network. The firewall is monitored by a third party vendor.

E. Log-in Monitoring

DEI should address how it will implement procedures that will monitor log-in attempts and report any discrepancies.

After three invalid attempts to log-in to the network the user is locked out and must contact Network Support staff to unlock the workstation. If the user cannot

remember their password, Network Support staff may re-set the password. Network Support staff verifies the identity of the individual prior to resetting of the passwords.

F. Password Management

DEI shall determine what procedures it must establish for password creation, change and safeguarding. For example, establishing a policy prohibiting posting passwords on post-it notes on monitors.

Every individual that accesses the network must create a unique password. It must be eight characters or more in length, and must meet at least three of the following conditions: upper case, lower case, number or symbol. Users are required to change their password every thirty (30) days, and the user cannot repeat a password used within the last twelve 30-day cycles. Passwords must remain in effect at least one day. Users are advised that passwords are confidential and should not be shared with other staff. At least every two months Network Support staff audit passwords to identify any weaknesses.

G. Security Incident Procedures DEI shall implement policies and procedures to address security incidents.

DEI shall identify and respond to suspected or known security incidents. DEI shall mitigate to the extent practicable, the harmful effects of security incidents that are known to the covered entity and to document security incidents and their outcomes.

When a security incident or deficiency is identified within program language within GHI or PB&R, IDMS staff is notified immediately and corrections to the GHI or PB&R system are made. A system tracking log is utilized to track problems identified with GHI or PB&R and their resolutions.

III. Contingency Plan Safeguards

DEI shall establish policies and procedures for responding to an emergency or other occurrence that damages systems containing E-PHI.

A. Data Backup Plan

DEI shall establish and implement procedures to create and maintain exact copies of E-PHI.

All information stored in the GHI or PB&R databases are backed up nightly to tape. The tapes are sent to an offsite facility every Friday. Tape backups that are sent offsite weekly are stored there for three weeks. After a tape has been stored for three weeks it is re-used, thereby limiting backup to three weeks activity. The

daily backup schedule may be altered in the event of additional work days being added to the work week. In addition to the daily tape backup, DEI also copies the GHI/PB&R databases to another server that is offsite, which is not the same location as the tape backups). Also, transaction log backups are completed throughout the work day so that in the event of a minor disruption that does not destroy hardware, we may restore to the last transaction log backup.

B. Disaster Recovery Plan

DEI shall establish procedures to restore any loss of data.

Tape backups and server backups are stored in two different locations offsite. We may utilize new hardware and restore using the backup server with loss of data limited to no more than one day's data. If the backup server was also destroyed we would utilize the offsite tape backup with a loss of data limited to no more than one week's data.

C. Emergency Mode Operation An emergency operations plan only involves those critical business processes that must occur to protect the security of E-PHI during and immediately after a crisis situation.

DEI shall establish procedures to enable continuation of critical business processes for protection of the security of E-PHI while operating in emergency mode.

In case of an emergency, DEI may physically move to the location of the backup server where DEI will have access to the GHI and PB&R databases. In the event the alternate location was destroyed, DEI would install hardware in a new location and restore it using backup tapes.

D. Testing and Revision Procedure

DEI shall implement procedures for periodic testing and revision of contingency plans.

The Disaster Recovery Plan is audited annually.

E. Applications and Data Criticality Analysis

DEI shall assess the relative criticality of specific applications and data in support of other contingency plan components.

GHI and PB&R are the most critical systems within the Department for Employee Insurance.

F. Evaluation

DEI shall perform technical and non-technical evaluation of the components of its security safeguards.

Evaluation is completed via quarterly reports from third party vendor and an annual report from the Kentucky State Auditor.

IV. Business Associate Contracts and Other Arrangements

DEI shall permit a business associate to create, receive, maintain, or transmit E-PHI on the its behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information in accordance with the other applicable provisions of the security rule.

Written Contract or Other Arrangement DEI shall require the covered entity to document the satisfactory assurances that it has received from its business associate through a written contract or other arrangement that meets the applicable requirements of the security rule.

Business associates with which DEI contracts are Humana Insurance Company, Express Scripts, Inc., PricewaterhouseCoopers, IDMS, and Thompson Reuters contracts with each of these entities specifically require full compliance with both HIPAA Privacy and HIPAA Security requirements.

V. Facility Access Controls and Safeguards

DEI shall implement policies and procedures to limit physical access to its electronic information system and the facility or facilities in which they are house, while ensuring that properly authorized access is allowed.

A. Contingency Operations

DEI shall establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency-mode operations plan.

In the event of a disaster or the need to operate in an emergency situation, Network Support staff will be responsible for restoring lost data. Only staff previously authorized to access E-PHI will participate in the restoration processes.

B. Facility Security Plan

DEI shall implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

DEI requires a code to be entered to gain access to the computer room. The Personnel Cabinet is in the process of issuing swipe cards to all employees. Employees will need swipe cards to gain access to their designated floor. All hallways and offices have locks. Keys are issued to employees for access. There

are cameras on the exterior of the building.

C. Access Control and Validation Procedures

DEI shall implement procedures based on a person's role or function to control and validate his or her access to facilities, including visitor controls and control of access to software programs for testing and revision.

Those individuals with access to GHI and PB&R are also granted access to software programs for testing and revision. Management staff determines the level of security as previously indicated.

D. Maintenance Records DEI shall document repairs and modifications to the physical components of a facility that are related to security.All repairs to workstations are completed by Network Support staff.

VI. Device and Media Controls

DEI shall govern the facility's receipt and removal of hardware and electronic media that contains E-PHI and the movement of these items into, out of, and within the facility.

A. Disposal

DEI shall address the final disposition of E-PHI and/or the electronic media on which it is stored.

Network Support staff runs Wipedisk three times on all hard drives before they are disposed of permanently. CD's are shredded and diskettes are manually destroyed.

B. Media Re-Use

DEI shall remove E-PHI from electronic media before the media are made available for re-use.

Network Support runs Wipedisk three times on all hard drives prior to their re-use. This is the standard recommended by the Department of Defense.

C. Accountability

DEI shall maintain a record of the movement of hardware and electronic media and any person responsible therefore. Network Support staff maintain a log of the location of all workstations.

D. Data Backup and Storage

DEI shall create a retrievable, exact copy of E-PHI, when needed, before movement of equipment.

All information stored in the GHI or PB&R databases are backed up nightly to tape. The tapes are sent to an offsite facility every Friday. Tape backups that are sent offsite weekly are stored there for three weeks. After a tape has been stored for three weeks it is re-used, thereby limiting backup to three weeks activity. The daily backup schedule may be altered in the event of additional work days begin added to the work week. In addition to the daily tape backup, DEI also copies the GHI/PB&R databases to another server that is offsite, which is not the same location as the tape backups). Also, transaction log backups are completed throughout the work day so that in the event of a minor disruption that does not destroy hardware, we may restore to the last transaction log backup.

VII. Access Controls

DEI shall have policies and procedures for electronic information systems that maintain E-PHI to allow access only to persons or software that have been granted access rights.

A. Unique User Identification

DEI shall assign a unique name and/or number for identifying and tracking user identity.

Each user is assigned a unique user ID for system wide access. The ID must be used in conjunction with the password. The same user ID is used to access GHI and PB&R but a different password is required.

B. Emergency Access DEI shall have procedures for obtaining necessary E-PHI

during an emergency. Emergency procedures do not differ from daily operation

procedures.

C. Automatic Logoff

DEI shall have electronic procedures to terminate an electronic session after a pre-determined time of inactivity.

After ten (10) minutes of idle time a password-protected screen-saver appears on all computers within DEI. Staff is advised to lock their screen whenever they leave their workstation.

VIII. Audit Controls

DEI shall have in place hardware, software, and/or procedural mechanisms that record and examine activity in those systems that store or use E-PHI. To record activity, GHI/PB&R creates notes when a record is updated and/or changed. When notes are created the following fields are populated and saved as a system file. MemberNum, PlanNum, NoteSeqNum, NoteDte, UserID, NoteActionCde, Reason Code Note, OE ConfirmationNum and UserName.

IX. Integrity Controls

DEI shall protect E-PHI from improper alteration, change or destruction.

System edits are built into DEI applications to identify missing, altered or invalid data. The GHI system performs numerous field level edits on the application's database information whenever an applicant submits a new application or a planholder changes data within an existing application. When a critical edit is tripped or error is identified, then the error is resolved before the applicant or planholder can submit the application or make changes to the plan. System edits are properly designed to prevent users from circumventing controls and further averts the risk of data validity as well as ensuring the overall reporting processes are functioning properly. The application logging feature of system edits must also be retained for 6 years.

X. Breach Procedures

Following a breach of unsecured protected health information DEI must send notification of the breach to affected individuals, the Secretary, U.S. Department of Health & Human Services (HHS) and, in certain circumstances, to the media. In addition, business associates must notify DEI that a breach has occurred.

A. Individual Notice

DEI shall notify affected individuals following the discovery of a breach of unsecured protected health information. DEI must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the DEI has insufficient or out-of-date contact information for 10 or more individuals, the DEI shall provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the DEI has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.

B. Media Notice

When DEI experiences a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, it shall provide notice to prominent media outlets serving the State or jurisdiction. Like individual notice, this media notification shall be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

C. Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), DEI shall notify the Secretary of breaches of unsecured protected health information. DEI will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

D. Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the DEI following the discovery of the breach. A business associate must provide notice to the DEI without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the DEI with the identification of each individual affected by the breach as well as any information required to be provided by the DEI in its notification to affected individuals.